UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/691,361	10/21/2003	Jeffrey Bruce Lotspiech	ARC920030093US1	1410

67232 7590 05/23/2008

CANTOR COLBURN, LLP - IBM ARC DIVISION
20 Church Street
22nd Floor
Hartford, CT 06103

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
05/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/691,361
Filing Date: October 21, 2003
Appellant(s): LOTSPIECH ET AL.

David A. Fox
Registration No. 38,807
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 14 March 2008 appealing from the Office action mailed 17 October 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

IBM Response to DVB-CPT Call for Proposals for Content Protection & Copy Management xCP Cluster Protocol October 19, 2001

6,965,883 Xu et al. 11-2005

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1, 4, 6-8, 11, 13-15, 98, and 99, are rejected under 35 U.S.C. 103(a) as being unpatentable over IBM Response to DVB-CPT Call for Proposals for Content & Copy Management: xCP Cluster Protocol (hereinafter IBM Oct. 2001) in view of Xu et al. US Patent No. 6,965,883 (hereinafter '883).

As per the first limitation of claim 1, **"A method for securely removing a device from at least one of a plurality of devices in a network while protecting a content from unauthorized use or distribution, the method comprising: calculating an encryption key for a protected content in the network, based at least in part on a list of the plurality of devices in the network"** is taught in IBM Oct. 2001 on page 7, paragraphs 4-5 "Each piece of content or each content stream in the home is protected with a unique key. These keys are called title keys. Each title key is encrypted with the master key for the particular home, called the binding key. To play content, a device reads the encrypted title key embedded in the content file and decrypts it with the binding key. Then, with the title key, the device decrypts the content itself. Thus, the binding key is important secret in a given network. It is calculated as the cryptographic hash of three quantities: the media key, the network's binding ID, and the network's authorization table. The media key is in turn, calculated from the media key block. This is the calculation that separates the compliant devices from the circumvention devices, and is the basis of the renewability in the system. If the media key block is up-to-date, no known circumvention device will be able to calculate the correct media key from it.", note the circumvent devices are interpreted to be equivalent to the removed device, the content is protected by encryption with an up to date key.

As per the second limitation, **"recalculating the encryption key for all devices remaining in the network and the protected content, using the modified list; and the authorization table"** is shown in IBM Oct. 2001 page 7, paragraph 9 "The binding key will change whenever: 1. A new device is introduced into the home (changing the authorization table)".

As per the third limitation, **"and reencypting the protected content with the recalculated encryption key"** is disclosed in IBM Oct. 2001 page 7, paragraph 10 "Every time the binding key changes, all devices in the cluster shall re-encrypt all title keys. To do this, a device must first decrypt the title key using the old binding key, and then re-encrypt it using the new binding key".

As per the fourth limitation, **"tentatively marking the device for removal, by modifying the list of the plurality of devices in the network, wherein the list of the pluraltiy of devies is included in an authorization table;** however '883 teaches "Group membership management 122 maintains the group membership information for every terminal on the same multicast link and is responsible for determining the join status of each terminal. Multicast security unit 123 is responsible for sending decryption key 118 to user terminal 110. Optionally, multicast security unit 123 may encrypt the multicast data from multicast server 190 before it is sent to user terminal 110. Multicast security unit 123 sends decryption key 118 when the user initially joins a multicast session. Multicast security unit 123 updates decryption key 118 either when another multicast user terminates the session or at discrete time intervals" in col. 7, lines 4-16.

As per the fifth limitation, **"the device marked for removal automatically acknowledging the removal"** however '883 teaches a device sending a message to be removed it is acknowledging its removal in col. 14, lines 12-20.

As per the sixth limitation, **"automatically recording the removal of the device in the authorization table"** however '883 teaches updating a database of authorized devices in col. 7, lines 4-16.

Regarding claim 4, **"wherein recalculating the encryption key comprises including a key management block in the calculation"** is taught in IBM Oct. 2001 page 7, paragraph 9.

Regarding claim 6, **"wherein recalculating the encryption key comprises including the binding identification for the plurality of devices, excluding the device to be removed"** is shown in IBM Oct. 2001 on page 7, paragraph 8.

Regarding claim 7, **"wherein the protected content is encrypted with a title key; and further comprising reencrypting the title key with the recalculated encryption key"** is disclosed in IBM Oct. 2001 page 7, paragraph 4.

Regarding claim 98, **"calculating the encryption key includes calculating the encryption key in response to a management key from a key management block, a binding ID associated with each of the devices on the list and a hash"** is taught in IBM Oct. 2001 page 7, paragraph 5.

Regarding claim 8, this claim is directed to the system performing the method of claim 1; therefore it is rejected along similar rationale.

Regarding claims 11, 13, 14, and 99, these claims contain substantially similar subject matter as claims 4, 6, 7, and 98; therefore they are rejected along similar rationale.

Regarding claim 15, **"wherein the plurality of devices comprise any one or more of: a television, a set top box, a personal video recorder, a video cassette recorder, a compact disk player, a compact disk player recorder, a personal computer, a portable music player, an audio player, a video player, a game console, and a personal network storage device"** is taught in IBM Oct. 2001 page 6 note the picture shows the plurality of devices.

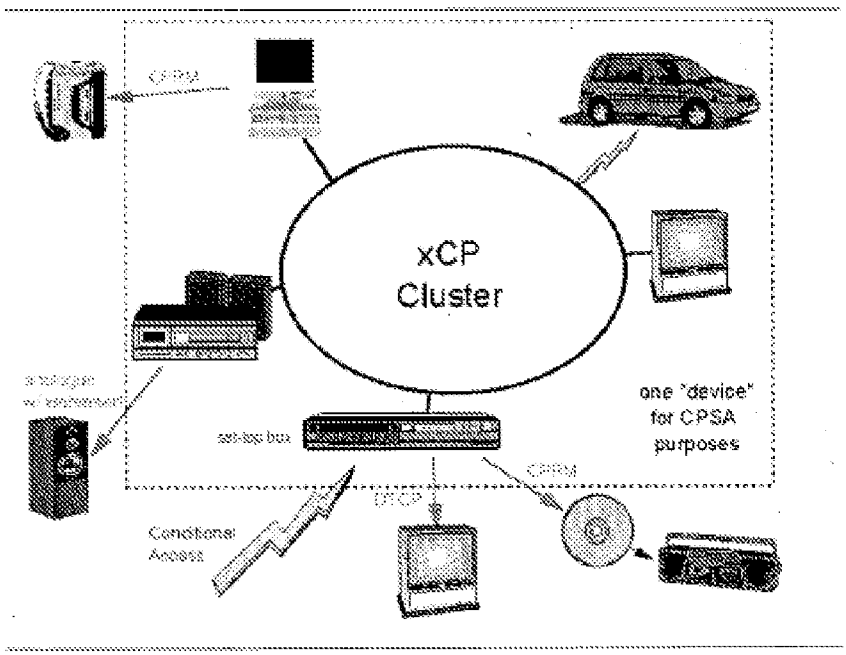

Figure 1 - Relationship of xCP Cluster to the Copy Protection System Architecture

(10) Response to Argument

Regarding appellant's argument beginning on page 3, "This rejection is traversed for the following reasons. Claim 1 recites, inter alia, "recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table." Neither IBM Oct. 2001 nor Xu teaches or suggests this feature. In applying the references the Examiner cites IBM Oct. 2001 as allegedly teaching this feature. The Examiner cites to page 7, paragraph 9 as teaching altering a binding key whenever a new device is introduced into the home. This is contrary to claim 1, which details a method of securely removing a device, not adding a device. The recalculating step in claim 1 is based on the modified list and the authorization table after a device is removed. The recalculating of claim 1, when properly read in light of the entire claim, is not taught by IBM Oct. 2001 as IBM Oct. 2001 deals with adding a device to a network, not removal".

The grounds of rejection stated above teach the invention. The references need to be reviewed for all they contain or suggest. IBM Oct. 2001 teaches a modified list to be also when a device is removed see page 7, paragraph 5, "Thus, the binding key is the important secret in a given network … This calculation that separates the compliant devices from the circumvention devices, and is the basis of the renewability in the system. If the media key block is up-to-date, no known circumvention device will be able to calculate the correct media key from it". Note the circumvent device is interpreted equivalent to 'removed devices' in addition the process of "updating" would account for removed / circumvent devices.

Regarding appellant's argument on page 4, "Further, IBM Oct. 2001 does not teach "recalculating the encryption key for all the devices remaining in the network and the protected content, using the modified list; and the authorization table." IBM Oct. 2001 makes reference to a media key, a network's binding ID and a network's authorization table. There is no teaching in IBM Oct. 2001 of using a list of devices in the network as part of the calculation of an encryption key when a user terminates a multicast session (column 7, lines 13-17). Xu fails to teach recalculating a decryption key using a modified list and an authorization table. Thus, even if IBM Oct. 2001 and Xu are combined, these features of claim 1 cannot be taught".

The grounds of rejection stated above teach the invention. On the IBM Oct. 2001 page 7, the reference teaches that the binding key is kept up to date. On page 10, of the IBM Oct. 2001 reference Figure 2 indicates that the Media Key Block is made up of the list of devices, in addition on page 11 it is explained that the authorization table which is hashed for the binding key calculation is an ASCII file that contains all of the positive responses for the "authorize me" messages that have occurred in the cluster, (i.e. this would be the current devices in a cluster).

Regarding appellant's argument on page 4, "The Examiner acknowledges that IBM Oct. 2001 fails to teach "tentatively marking the device for removal, by modifying the list of the plurality of devices in the network, wherein the list of the plurality of devices is included in an authorization table." The Examiner relies on Xu teaching this feature. Appellants respectfully disagree. Xu broadly teaches updating a decryption key when a device terminates a session or at discrete intervals (column 7, lines 13-16). There is no reference that a device is marked for removal or that the device is being removed from the network. The device has terminated a session, not been removed from the network. Nor is there any teaching of modifying a list of devices that is included in an authorization table. The description of updating the decryption key discussed in Xu is sparse and simply does not include the features of claim 1. Thus, even if IBM Oct. 2001 and Xu are combined, the features of claim 1 do not result".

The grounds of rejection stated above teach the invention. The references should be reviewed in combination for all they contain. Xu teaches 'tentatively marking a device for removal' by indicating a start and stop of a user terminal session. In addition Xu teaches that a user terminal can extend the stop time; therefore if a user does not extend the stop time they are acknowledging removal. Note when the session is terminated the device is removed from the network. The authorization table is taught in IBM Oct. 2001.

Regarding appellant's argument on page 5, "Claims 98 and 99 recite "calculating the encryption key includes calculating the encryption key in response to a management key from a key management block, a binding ID associated with each of the devices on the list and a hash of an authorization table listing authorized devices." It is important to note that claims 98 and 99 recite that the hash is on the authorization table, not on all the elements (i.e., management key, binding ID, and authorization table) used to compute the encryption key. In applying the references, the Examiner cites to page 7, paragraph 5 of IBM Oct. 2001. This section of IBM Oct. 2001 teaches computing a key based on a hash of three quantities: the media key, the network's binding ID

and the network's authorization table. Claims 98 and 99, however, only recite using the hash of the authorization table, not all three quantities. Thus, IBM Oct. 2001 does not teach the elements of claims 98 and 99".

The grounds of rejection stated above teach the invention. As indicated by appellant IBM Oct. 2001 teaches calculating the encryption key … with … a hash of an authorization table listing authorized devices. The fact that IBM Oct. 2001 cites more than the required claim does not preclude the reference from being utilized as part of a 103 rejection to show that this limitation is available in the prior art. The references need to be looked at in combination for all they contain or suggest. In addition on page 11, section 5.2 The Binding Key – "The binding key is calculated using the binding ID, the media key, and the hash of the authorization table as follows:" Therefore, Appellant's argument is not precise with the IBM Oct. 2001 document, which teaches calculating the binding key with the hash of the authorization table as well as using the media key and the binding ID not hashed.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/ELLEN TRAN/

Primary Examiner, Art Unit 2134

Conferees:

/KIMYEN VU/

Supervisory Patent Examiner, Art Unit 2135

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134